ADAMS ML052920123

| Yes __ No __ Make Public After President Submits Budget *(For OIS Use Only)* |
|---|

# U.S. Nuclear Regulatory Commission
# Privacy Impact Assessment

***Instructions:*** ***Section A, B, C, and D must be completed for all systems. Section E must be completed if yes is the answer to Section B, questions 1 and 2.***

Date: 10/12/2005

## A. GENERAL SYSTEM/APPLICATION INFORMATION

(See definitions at end of document)

1. Person completing this form:

| Name | Title | Phone No. | Office |
|---|---|---|---|
| Cynthia G. Harbaugh | Sr. Security Specialist | 415-7050 | ADM |

2. System owner:

| Name | Title | Phone No. | Office |
|---|---|---|---|
| Mark D. Lombard | Chief, Security Branch | 415-7404 | ADM |

3. What is the name of this system?

   Access Control and Computer Enhanced Security System /Photo Identification Computer System (ACCESS/PICS)

4. Briefly describe the purpose of this system. What agency function does it support?

   The ACCESS monitors and controls building and area access through card readers and alarms at the NRC White Flint Complex. The PICS, a sub system to ACCESS, manufactures and programs photo-identification badges used for personal identification, clearance verification and for building/area access via card readers at Headquarters and the regional offices. Data collected to support this system is covered by NRC Privacy Act System of Records; NRC-40, “Facility Security Access Control.” Access to this information is limited to those with an official need-to-know for the information.

5. Does this Privacy Impact Assessment support a proposed new system or a proposed modification to an existing system.

_____New System __X___ Modify Existing System

## B. PRIVACY ACT APPLICABILITY

1. Does this system collect, maintain, or disseminate personal information in identifiable form (e.g., name, social security number, date of birth, home address, etc.) about individuals ?

   Yes __X__ No ___

   Information is collected from Federal employees, contractors, and a limited number of members of the public (day care center parents and guardians).

2. If yes, will the data be retrieved by an individual's name or other personal identifier (e.g., social security number, badge number, etc.)?

   Yes __X__ No ____

**If you answer yes to questions 1 and 2, complete Section E.**

## C. INFORMATION COLLECTION APPLICABILITY

1. Will the personal data be collected from or maintained by persons who are not Federal employees?

   Yes __X__ No_____

2. Will the data be collected from Federal contractors?

   Yes __X__ No _____

3. If the answer is yes to either question 1 or 2, will the data be collected from 10 or more persons during a calendar year?

   Yes __X__ No ____

4. If the answer is yes to question 3, is the information to be collected covered by an existing OMB clearance number? If yes, indicate the clearance number,

   Standard Forms SF-86, "Questionnaire for National Security Positions;" SF-85, "Questionnaire for Non-Sensitive Positions;" and SF-85P, "Questionnaire for Public Trust Positions" have been approved by OMB under OMB clearance number 3206-0005 and are used to collect the bulk of the information.

## D. RECORDS RETENTION AND DISPOSAL SCHEDULE APPLICABILITY

Does this system already have a NARA-approved records disposition schedule? (Reference NUREG-0910, "NRC Comprehensive Records Disposition Schedule," or contact your office Records Liaison Officer or John Harris, OIS.)

Yes X No ____

If yes, list the records schedule number GRS 1, 18, and 20 reference NRC.

***Complete Section E only if the answers to Section B, questions 1 and 2 are Yes.***

## E. SYSTEM DATA INFORMATION

1. *Type* of information maintained in the system

   a. Describe the information to be maintained in the system (e.g., financial, medical, training, personnel.) Give a detailed description of the data.

   NRC employees' and contractors' demographic data, personal identification, and clearance/access approval information, to include but not limited to: social security number, identity verification information (image), credential (badge category) information and building/area access permitted.

   **Only the names** of day care center parents and guardians are maintained for the purpose of issuing them a non-photo access card to enter the day care facility.

2. *Source* of the data in this system

   a. Are data being collected from the subject individual? If yes, what types of data are being collected?

      Yes, the personal data as reflected in 1.(a) above is collected from the subject individual personally.

   b. Are data on this individual being collected from other NRC files and databases for this system? If yes, identify the files and databases.

      Yes, some of the data identified in 1.(a) above are derived from the Integrated Personnel Security System.

   c. Are data on this individual being collected from a source or sources other than the subject individual and NRC records? If yes, what is the source and what type of data is being collected?

      No.

d. How will data collected from sources other than the subject individual or NRC records be verified as current, accurate, and complete?

N/A.

3. *Attributes* of the data

a. Are the *data elements* described in detail and documented? If yes, what is the name of the document? Where is it located?

Yes, the data elements are described and documented in COTS User's and Administration manuals.

b. Is the use of the data both relevant and necessary for the purpose for which the system is designed?

Yes.

c. Will the system derive (i.e., create) new data or create previously unavailable data about an individual through aggregation from the information collected?

No.

(1) How will aggregated data be maintained, filed, and utilized?

N/A

(2) How will aggregated data be validated for relevance and accuracy?

N/A

4. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

System includes password and "rights" protection; certain data fields include automatic validation/integrity checks.

5. How will the data be *retrieved* from the system?

a. Can it be retrieved by personal identifier? Yes _X_ No ___
If yes, explain.

Data can be retrieved by name, social security number, badge number or employer.

b. Is a password or data description required? Yes _X_ No ___
If yes, explain.

The system uses password and specific "rights" protection to ensure

access to only those data elements where the individual accessing the system has a need-to-know and/or need to modify information privileges.

6. Describe the report or reports that can be produced from this system.

   a. What reports are produced from the system?

      The system can produce numerous specific yet generic reports systems such as: all active badges; badges by category; specific badge issuance/use history.

   b. What are the reports used for?

      Reports will be used for security information, budgetary purposes, resource planning, and quality control purposes.

   c. Who has access to these reports?

      The Security Branch Staff and the ADM system administrator/ IT Coordinator.

7. *Records retention*

   a. What are the record types contained in this system and the medium on which they reside? (Examples: type - program records, medium - electronic; type - database, medium - electronic; type - system documentation, medium - paper.)

      As listed in the NRC Privacy Act System of Records Notice for NRC-40, “Facility Security Access Control Records.”

   b. What is the NARA-authorized retention period for each records series in this system?

      As listed in the NRC Privacy Act System of Records Notice for NRC-40, “Facility Security Access Control Records.”

   c. If unscheduled, what are your retention requirements for each records series in this system?

      N/A

   d. What are the procedures for disposing of the data at the end of the retention period (specifically address paper copy, magnetic, or other forms of media)?

      Records are considered to be Official Use Only and are destroyed in accordance with NRC policy as specified in Management Directive 12; by approved shredders for paper and methods ensuring total destruction for electronic media.

e. How long will produced reports be maintained?

Specific reports are maintained until no longer needed; or system records as prescribed in the NRC Privacy Act System of Records Notice.

f. Where are the reports stored?

Reports are generally considered to be Official Use Only and are stored in accordance with NRC policy as specified in Management Directive 12 (in locked cabinets if deemed necessary based on the specific report) or as specified by NRC Privacy Act System of Records Notice, whichever is more restrictive.

g. Where are the procedures for maintaining the data/reports documented?

Procedures for maintaining the data/reports will be documented in internal procedures.

h. How will unused or unwanted reports be disposed of?

Records are considered to be Official Use Only and are destroyed in accordance with NRC policy as specified in Management Directive 12; by approved shredders or disposal methods (i.e., Classified and Sensitive Unclassified Waste Only containers).

8. Capability to *monitor individuals*

a. Will this system provide the capability to identify, locate, and monitor (e.g., track, surveillance) individuals? Yes _X_ No __.
If yes, explain.

A limited "tracking" capability exists based on an individual's use of their photo-identification badge through the access control/card reader system.

b. What controls will be used to prevent unauthorized monitoring?

Specific reports and system queries are required to monitor the use of a given badge. Access to run these reports/queries is held to a limited number of people with a need-to-know this information for security/investigative purposes.

9. Coverage Under Existing *Privacy Act System of Records*

a. Under which Privacy Act System of Records (SOR) notice does this system operate (link to list of SOR available on NRC Internal Home Page)? Provide number and name.

NRC-40, "Facility Security Access Control Records."

b. If the Privacy Act System of Records is being modified, will the SOR

notice require amendment or revision? ___ Yes _X__ No.
If yes, explain.

10. *Access* to the Data

a. Who will have access to the data in the system (users, managers, system administrators, developers, other)?

System administrators, ADM IT Coordinator, Security Branch Chief and the Security Branch staff have full access to the system.

b. Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where?

Yes, criteria, procedures, controls and responsibilities are documented in the ACCESS/PICS Security Plan and the COTS User's and Administration guides. Internal policy and procedures are being developed to address the handling and control of privacy act information.

c. Will users have access to all data in the system or will users' access be restricted? Explain.

There are multi-level access privileges (full control, limited control, view only).

d. What controls are or will be in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

There are only four terminals that can access the system, each of which are in controlled locations this combined with the very limited number of individuals having access to the system and the multi-level access controls significantly reduces the vulnerability of the data to misuse.

e. Do other systems share data or have access to data in this system?
Yes ___ No __X__. If yes, explain.

f. Will other agencies share data or have access to data in this system (Federal, State, local, other)? Yes ___ No _X_. If yes, explain.

g. Were Privacy Act clauses cited (or will be cited) and were other regulatory measures addressed in contracts with contractors having access to this system?
Yes __X__ No ___. If yes, explain.

Appropriate security clauses will be included in the contract (s). Individual's are required to sign an NRC Security Acknowledgment which stipulates their agreement to protect sensitive unclassified (OUO/privacy) information.

DEFINITIONS

Personal Information is information about an identifiable individual that may include but not be limited to:

- race, national or ethnic origin, religion, age, marital or family status
- education, medical, psychiatric, psychological, criminal, financial, or employment history
- any identification number, symbol, or other particular assigned to an individual
- name, address, telephone number, fingerprints, blood type, or DNA

Aggregation of data is the taking of various data elements and then turning them into a composite of all the data to form another type of data such as tables or data arrays, or collecting data into a single database.

Consolidation means combining data from more than one source into one system, application, or process. Existing controls for the individual parts should remain or be strengthened to ensure no inappropriate access by unauthorized individuals. However, since individual pieces of data lose their identity, existing controls may actually be diminished; e.g., a summary census report may not point at the individual respondent but rather at a class of respondents, which makes it less personal.

**PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL**
*(For Use by OIS Staff)*

**System Name:** Access control and Computer Enhanced Security System/Photo Identification Computer System (ACCESS/PICS)

**Submitting Office:** Office of Administration

## A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

__X__ Privacy Act is applicable. Currently covered under System of Records NRC-40. No modification to the system notice is required.

____ Privacy Act is applicable. Creates a new system of records. FOIA/PA Team will take the lead to prepare the system notice.

____ Privacy Act is applicable. Currently covered under System of Records, NRC _____. Modification to the system notice is required. FOIA/PA Team will take the lead to prepare the following changes:

**Comments:**

ACCESS/PICS is covered by Privacy Act system of records NRC-40, "Facility Security Access Control Records." The only information maintained about members of the public are the names of the day care center parents and guardians for the purpose of issuing them a non-photo access card to enter the day care facility.

| Reviewer's Name | Title | Date |
|---|---|---|
| Sandra S. Northern | Privacy Program Officer | October 20, 2005 |

## B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

____ No OMB clearance is needed.

____ OMB clearance is needed.

__X__ Currently has OMB Clearance.

**Comments:**

The information collected for the Access Control and Computer Enhanced Security

System/Photo Identification Computer System (ACCESS/PICS) on forms SF-85, SF-85P, and SF-86 is covered by the Office of Personnel Management's OMB Clearance number 3206-0005.

| Reviewer's Name | Title | Date |
|---|---|---|
| Christopher J. Colburn | Team Leader<br>Information Collections Team | October 25, 2005 |

**C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION**

____ Additional information is needed to complete assessment.

__X__ Needs to be scheduled.

____ Existing records retention and disposition schedule covers the system - no modifications needed.

____ Records retention and disposition schedule must be modified to reflect the following:

**Comments:**

The Records and Archives Services Section (RASS) has reviewed the ACCESS/PICS PIA. Based on your reference to the retention and disposal segment of NRC Systems of Records 40, we agree that the system database appears to be covered by NARA's General Records Schedules. However, the system inputs and outputs are not clearly scheduled, and the retention period is not definitively specified. The PIA can be improved by citing the specific schedule numbers referenced in PIA Section D. Similarly, a more specific retention period should be identified for each category of records that can be implemented into system design. It is insufficient to specify, for example, that the information will be destroyed when 2 years old or when no longer needed, which ever is later. We need to develop specific retention periods for implementing into system design, that meets your retention requirements and that falls within this range.

Although the value of the records related to the NRC ID Badges and visitor log information contained in the system appears to be reflected correctly in NRC System of Records 40, we believe that the system needs to be evaluated further by a management analyst to consider the scheduling of the system in a more holistic manner that includes the specific inputs and how long each are maintained, a more specific listing of the records series actually maintained in the system and how long they are maintained, and a list of the specific outputs/reports and their retention periods. This will ensure that the actual categories of system data, inputs, and outputs are properly scheduled and the retention periods linked to the periods contained in the existing General Records Schedules.

Managing the system according to a variety of disposition instructions, as we have here, would be improved with a single records disposition schedule that covers all of the components to

more clearly encompass all inputs, outputs and data. This supports the current NARA guidance to schedule systems along with their inputs and outputs. The scheduling process will also help identify unique information, its life cycle, and when the information should be destroyed.

We request the system contact to submit NRC Form 616, "Notification of Electronic System Design or Modification," and NRC Form 637, "NRC Electronic Information System Records Scheduling Survey," to help identify the system recordkeeping requirements and initiate the records scheduling process for the system and its data.

In accordance with the NARA regulations at 36 CFR 1234.20(a), the resulting recordkeeping requirements and NARA approved disposition instructions must be built into the systems design. Please note that system data cannot be destroyed except in accordance with a NARA approved records disposition schedule.

Also note in Section E, Items 7.a and b, that there are several types of records associated with the system for which some have NARA approved records schedules. These are shown in the table, below.

7.a & b. Record types, medium, and NARA-authorized retention period for each.

| Type | Medium | Schedule & Retention Period |
|---|---|---|
| Program (Software) | Electronic | GRS 20-10, "Special Purpose Programs." Delete when related master file or database has been deleted or when software program is superseded, and is no longer needed to access legacy records. |
| Inputs, Outputs, and Database | Electronic | Unscheduled. Retention periods and disposition instructions to be based on the GRS schedules that apply to the various data. |
| System Documentation (Data systems specifications, data dictionairy, user guides) | Electronic & Paper | GRS 20-11.a, "Documentation." Destroy or delete when superseded or obsolete, or upon authorized deletion of the related master file or data base, or upon the destruction of the output of the system if the output is needed to protect legal rights, whichever is latest. |
| **Copies** of System Documentation Related to the Security Plan | Electronic & Paper | GRS 20-11.b, "Documentation." Destroy or delete when superseded or obsolete. |

RASS through its Records Management Policy and Compliance contractor will work with ADM to identify the proper retention requirements that can be implemented in the system to control each series in the system for their life cycles.

| Reviewer's Name | Title | Date |
|---|---|---|
| John Harris | Chief, Records and Archives Services Section, RFPSB, IRSD, OIS | 10/27/05 |

**D. BRANCH CHIEF REVIEW AND CONCURRENCE**

___ Does not constitute a Privacy Impact Assessment required by the E-Government Act of 2002.

_X_ Does constitute a Privacy Impact Assessment required by the E-Government Act of 2002 and requires approval of the Director, IRSD.

CONCUR IN REVIEW: /RA/ Date 10/27/05
Brenda J. Shelton, Chief
Records and FOIA/Privacy Services Branch

**E. DIVISION DIRECTOR APPROVAL OF PRIVACY IMPACT ASSESSMENT:**
*(Approval is only required when Yes is given to Section B, questions 1 and 2 and Section C, question 1. The system collects, maintains, or disseminates personal information in identifiable form about members of the public.)*

/RA/ Date: 10/ 27/05
John J. Linehan, Director, Information and Records Services Division

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/**
**PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

| | | |
|---|---|---|
| **TO: (Sponsoring Office)**<br>Office of Administration | **Office Sponsor:**<br>Mark D. Lombard, Chief<br>Security Branch | |
| Reginald Mitchell, Director<br>Business Process Improvement and Applications Division, OIS | **Name of System:** Access Control and Computer Enhanced Security System /Photo Identification Computer System (ACCESS/PICS) | |
| Charlotte Turner, Director<br>Program Management, Policy Development, and Analysis Staff, OIS | **Date Received:** 10/14/2005 | **Date Completed**:<br>10/27/05 |

**Noted Application Development and System Security Issues:**

1. The system, its data, and unique inputs and outputs are not clearly covered by National Archives and Records Administration (NARA) approved records disposition schedules, and require going through the records scheduling process. The schedules should reflect specific periods for the appropriate information based on the authorized disposition stated in the NARA General Records Schedules that are referenced in the NRC System of records number 40.

2. The ADM Project Manager is requested to submit to CPIC@nrc.gov NRC Form 616, "Notification of Electronic System Design or Modification," and NRC Form 637, "NRC Electronic Information System Records Scheduling Survey," to help describe and categorize all system data, inputs and outputs, and to identify recordkeeping requirements and initiate the records scheduling process for the system and its data. The Project Manager shall also work with the Records and Archives Services Section (RASS) staff to ensure that the proper records management functionality and NARA records schedules are planned and developed, as appropriate.

3. Until all series of system data, and unique system inputs and outputs are covered by NARA approved records disposition schedules, they must be retained as though they were permanent material.

4. The System Project Manager shall complete an NRC Form 306, "Files Maintenance and Disposition Plan," for the system components identified in the Section C. comments. In Column 6.D, "Disposition," the plan shall reflect for system inputs, outputs, and database, the statement, "Unscheduled. This material is currently unscheduled and must be retained until the National Archives and Records Administration (NARA) approves a records disposition schedule for this material." Obtain the ADM Records Liaison Officer (RLO) signature (Susan Bellosi) and ensure the required distribution; e.g., Project Manager, RLO, and the NRC Records Officer (Brenda Shelton).

5. The RASS through its Records Management Policy and Compliance contractor will work with ADM to evaluate and identify the proper retention requirements that can be implemented in the system to control each series in the system for their life cycles.

6. In accordance with the NARA regulations at 36 CFR 1234.20(a), the resulting recordkeeping requirements and NARA approved disposition instructions must be built into the systems design and the implementation of approved disposition instructions documented through the user manual, system documentation, or other evidence.

| | | |
|---|---|---|
| Brenda J. Shelton, Chief<br>Records and FOIA/Privacy Services Branch, OIS | Signature: /RA/ | Date:10/27/05 |